IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

JOHNNA BATTLES, individually and on behalf of all others similarly situated, ***Plaintiff*,** **v.** **AFFINITY CARDIOVASCULAR SPECIALISTS, LLC, d/b/a ALABAMA CARDIOLOGY GROUP** ***Defendant.***	**Case No.:_____** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Johnna Battles, ("Plaintiff") brings this Class Action Complaint against Defendant Affinity Cardiovascular Specialists, LLC, doing business as, Alabama Cardiology Group, ("Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

STATEMENT OF FACTS

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the protected health information ("PHI") and other personally identifiable information ("PII") of its patients and employees, including, but not limited to: name, address, email, phone number, date of birth, social security number, health insurance information, medical information (dates of service, diagnoses, medications, imaging, lab results, etc.), driver's license numbers, credit/debit card information, and bank account numbers.

2. While providing a health care service, Defendant collects, creates, or shares information about health status, the provision of health care, or payment for health care that can be used to identify an individual.

3. Medical records represent the most sensitive information available concerning a person's private affairs. These records reveal intimate and personal aspects of the human condition, such as illnesses that might carry social stigma and details about substance abuse, family planning and mental health. Congress has passed legislation under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to protect this highly confidential data, because in the wrong hands, bad actors may target and exploit the most sensitive and vulnerable populations among the public.

4. Defendant's published privacy policy provides, "[w]e are required by law to maintain the privacy of your protected health information. . . .We have set up reasonable safeguards that protect against impermissible uses and disclosures and limits incidental uses or disclosures."[1]

5. On, or about, July 2, 2024, Defendant detected unusual activity on its computer network and determined that Plaintiff's personal information—which was entrusted to Defendant on the mutual understanding that Defendant would protect it against unauthorized disclosure—was accessed and exfiltrated by unauthorized parties (hereafter referred to as the "Data Breach"). The unauthorized parties gained access to Defendant's network on June 6, 2024, and maintained access to the network until detected on July 2, 2024.[2]

[1]Alabama Cardiovascular Group, *Notice of Privacy Practices*, effective April 14, 2003, available here: http://alcardio.com/privacy.html
[2]*See,* Notice of Data Security Incident, https://www.acgsecurityincident.com

6. On, or about, August 2, 2024, Defendant sent out data breach notice letters to individuals who were affected by the data breach. Omitted from the data breach notice letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff, who retains a vested interest in ensuring that her PHI/PII remains protected.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's data was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the information from those risks left the data in a dangerous condition.

8. The Data Breach was a direct result of Defendant's failure to implement reasonable safeguards to protect PHI/PII from a foreseeable and preventable risk of unauthorized disclosure. Had Defendant implemented administrative, technical, and physical controls consistent with industry standards and best practices, it could have prevented the Data Breach.

9. Defendant's conduct resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PHI/PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PHI/PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. Plaintiff suffered actual injury in the form of the unauthorized disclosure the PHI/PII that was compromised in the Data Breach. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

10. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

11. "Data breaches in healthcare have reached alarming levels, with the Office of Civil Rights reporting 725 notifications of breaches in 2023, where more than 133 million records were exposed or impermissibly disclosed."[3] Plaintiff faces a substantial risk of future medical identity theft or fraud where Plaintiff's unique medical identifying information was obtained by cybercriminals in a targeted attack. Medical identity theft involves the misuse of a person's unique medical identity to wrongfully obtain health care goods, services, or funds.[4] Medical identity theft "can result in bills for procedures the patient has never had, inaccurate medical records, and potentially life-threatening care."[5]

12. Typically, hackers sell the personal information in medical records "to criminals who create phony providers to submit fraudulent claims on a mass scale that can result in hundreds of millions of dollars in Medicaid, Medicare, or other insurance fraud."[6]

13. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation. The circumstances demonstrating a substantial risk of future exploitation include, but are not limited to:

a. **Sensitive Data Type**: The data acquired in the Data Breach included unencrypted names, dates of birth, non-truncated social security numbers, health insurance information, medical information, driver's license numbers,

---

[3] *Healthcare fraud and the burden of medical ID theft*, available at: https://www.experian.com/blogs/healthcare/healthcare-fraud-and-the-burden-of-medical-id-theft/

[4] *See*, *Common Types of Health Care Fraud*, Center for Medicare & Medicaid Services (CMS) Fact Sheet, available at: https://www.cms.gov/files/document/overviewfwacommonfraudtypesfactsheet072616pdf

[5] *Healthcare fraud and the burden of medical ID theft*, available at: https://www.experian.com/blogs/healthcare/healthcare-fraud-and-the-burden-of-medical-id-theft/

[6] *Someone could steal your medical records and bill you for their care.* https://www.npr.org/sections/health-shots/2023/07/26/1189831369/medical-identity-fraud-protect-yourself

credit/debit card information, bank account numbers and passwords. Upon information and belief, this category of data is used by cybercriminals to perpetuate fraud, identity theft, and other forms of exploitation.[7]

b. **Data Misuse**: Upon information and belief, the data acquired in the Data Breach was leaked on the dark web. The dark web uses a series of encrypted networks to hide users' identities, which makes it convenient for criminals to buy and sell illegally obtained data. Many criminals purchase stolen personal data off the dark web before launching social engineering-based attacks. A social engineering attack is a method of using psychological manipulation to deceive a victim and gain access to a computer system or to steal sensitive information such as login credentials. Social engineering attacks that can be launched using names, telephone numbers and email addresses include phishing, smishing (SMS message), vishing (voice messaging), pretexting, and baiting attacks.

14. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PHI/PII in its custody, and has created a separate, particularized, and concrete harm to the Plaintiff.

15. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused them to: (i) spend money on mitigation measures like credit monitoring services and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff's suffered can be redressed by a favorable decision in this matter.

16. Plaintiff faces a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a cybercriminal, known for stealing and reselling personal data on the dark web. Names, telephone numbers and email addresses can be used by cybercriminals to launch social engineering attacks designed to trick individuals into giving away sensitive information. Plaintiff has incurred

[7] https://www.f-secure.com/us-en/articles/why-do-hackers-want-your-personal-information

out of pocket costs for purchasing products to protect from phishing, smishing (SMS message), vishing (voice messaging), pretexting, and other social engineering-based attacks.

17. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft and can, in the future, commit a variety of crimes including, opening new financial accounts, taking out loans, using Plaintiff's information to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PHI/PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

19. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach.

20. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PHI/PII was accessed during the Data Breach.

21. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

22. Defendant is covered by HIPAA (*see* 45 C.F.R. §160.102) and as such is required to comply with the HIPAA Privacy Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

23. The HIPAA Privacy Rule and Security Rule establishes standards for the protection of protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a covered entity. *See* 45 C.F.R. § 160.103.

24. The Privacy Rule requires Defendant to implement appropriate safeguards to protect the privacy of protected health information. The Security Rule requires Defendant to implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The HIPAA rules also require Defendant to provide notice of an unauthorized disclosure of unencrypted protected health information, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

25. In the course of their relationship, Defendant collected or created PHI/PII related to Plaintiff and Class Members.

26. Defendant was obligated to use reasonable technical, administrative, and physical safeguards to protect the PHI/PII it collected or created. This obligation was contained in the applicable privacy policy and through other statutory privacy requirements.

27. Plaintiff and the Class Members (later defined) relied on Defendant's representations and on this sophisticated business entity to keep their PHI/PII confidential, securely maintained, and to make only authorized disclosures of this information.

Data Breaches Are Avoidable

28. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the data from those risks left the data in a dangerous condition.

29. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement reasonable data protection measures for the collection, use, disclosure, and storage of PHI/PII; and/or (iv) ensure its third-party vendors were required to implement reasonable data protection measures consistent with Defendant's data protection obligations.

30. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[8] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal posts portions of the data to increase their leverage and force the victim to pay the

[8] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).

ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[9]

31. Upon information and belief, the Data Breach involved the exploitation of known vulnerability or a phishing attack. A phishing attack involves the use of fraudulent emails, social media messages, text messages, websites, or other communication to trick people into revealing login credentials or other sensitive information. Phishing attacks are prevalent because they exploit human vulnerabilities. Cybercriminals can use phishing attacks to "trick people who have authorized access to their target—be it money, sensitive information or something else—into doing their dirty work."[10]

32. The Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), has issued guidance documents regarding compliance with the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.[11]

33. To detect and prevent cyber-attacks, Defendant could and should have implemented administrative, physical, and technical safeguards including, but not limited to, the following:

Administrative Safeguards

---

[9] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

[10] *What is phishing?* IBM security topics, https://www.ibm.com/topics/phishing (accessed June 11, 2024).

[11] *See*, U.S. Department of Health & Human Services, Security Rule Guidance Material, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

a. Implement policies and procedures to prevent, detect, contain, and correct security violations.

b. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the Defendant.

c. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

d. Apply appropriate sanctions against employees who fail to comply with the Defendant's security policies and procedures.

e. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

f. Identify a security official who is responsible for the development and implementation of the Defendant's policies and procedures to prevent, detect, contain, and correct security violations.

g. Implement procedures: (i) for the authorization and/or supervision of employees who work with electronic protected health information or in locations where it might be accessed; (ii) to determine whether an employee's access to electronic protected health information is appropriate; and (iii) for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.

h. Implement policies and procedures that, based upon the Defendant's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

i. Implement a security awareness and training program for all members of Defendant's workforce, including procedures for guarding against, detecting, and reporting malicious software.

j. Implement policies and procedures to address how the Defendant will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, known harmful effects of security incidents; and document security incidents and their outcomes.

k. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information.

l. Perform a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of electronic protected health information.

m. Contractually obtain satisfactory assurances that business associates will appropriately safeguard electronic protected health information.

n. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

o. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

p. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

Physical Safeguards

q. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

r. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

s. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Technical Safeguards

t. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

u. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

v. Implement a mechanism to encrypt and decrypt electronic protected health information.

w. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

x. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

y. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.

z. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.

aa. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments

may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

bb. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

cc. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

dd. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

ee. Configure firewalls to block access to known malicious IP addresses.

ff. Set anti-virus and anti-malware programs to conduct regular scans automatically.

gg. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

hh. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.

ii. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

jj. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

kk. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

ll. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

mm. Execute operating system environments or specific programs in a virtualized environment.

nn. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

oo. Conduct an annual penetration test and vulnerability assessment.

pp. Secure your backups.[12]

qq. Identify the computers or servers where sensitive personal information is stored.

rr. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch

[12] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

ss. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

tt. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

uu. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

vv. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

ww. To detect network breaches when they occur, consider using an intrusion detection system.

xx. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[13]

34. Given that Defendant collected, used, and stored PHI/PII, Defendant could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

35. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class Members' PHI/PII.

36. Defendant knew and understood unencrypted PHI/PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PHI/PII and of the

[13] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

37. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct.

38. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their names, social security numbers, and dates of birth were targeted by a sophisticated hacker. The substantial risk of future identity theft and fraud created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

39. Furthermore, Plaintiff and Class Members face a substantial risk of future spam, phishing, or other attacks designed to trick them into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime, where their names and contact information were acquired in the Data Breach and subsequently released on the dark web. The substantial risk of future exploitation created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

40. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[14] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

[14] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas*

41. Given the type of targeted attack in this case, the sophistication of the criminal responsible for the Data Breach, the categories of data involved in the Data Breach, typical hacker behaviors in similar data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been placed, or will be placed, on the dark web, it is reasonable for Plaintiff and the Class Members to assume that their PHI/PII was obtained by, or released to, criminals intending to utilize the data for future identity theft-related crimes or exploitation attempts.

42. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

43. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[15]

Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

[15] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

44. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

45. As a result of the Data Breach, Plaintiff's and Class Members' PHI/PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PHI/PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

46. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[16] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[17] Sensitive PII can sell for as much as $363 per record.[18] Further, a stolen medical identity has a $50 value on the black market.[19]

47. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their PHI/PII, and then permitting the unauthorized disclosure of the information, Plaintiff and Class Members were deprived of the benefit of their bargain.

---

[16] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[17] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[18] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] Study: Few Aware of Medical Identity Theft Risk, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm

48. The healthcare industry is hit hardest by cybersecurity threats. Unfortunately, patients typically end up paying for these incidents in the long run. "When asked how they're dealing with these costs, more than half of [healthcare] organizations said they are passing [the costs] on to customers."[20]

49. When agreeing to pay Defendant for products or services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

50. Through this Complaint, Plaintiff seeks redress individually, and on behalf of all similarly situated individuals, for the damages that resulted from the Data Breach.

JURISDICTION & VENUE

51. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant. Plaintiff is an Alabama citizen and at least 27 members of the class are citizens of the Commonwealth of Massachusetts.[21]

52. This Court has personal jurisdiction over Defendant because Defendant, as a member-managed limited liability company, takes the citizenship of its members. Defendant's

---

[20] *Alabama security breach exposes personal information of cardiologists, heart patients*, Cardiovascular Business, August 14, 2024, https://cardiovascularbusiness.com/topics/health-it/cybersecurity/alabama-security-breach-exposes-personal-information-cardiologists-heart-patients

[21] *See*, Breach Number 2024-1412, *Data Breach Notification Report,* Massachusetts Office of Consumer Affairs and Business Regulation, available here: https://www.mass.gov/doc/data-breach-report-2024/download

Executive Vice President and Secretary, Rachel A. Seifert, is a resident citizen of Franklin, Williamson County, Tennessee.

53. Venue is proper under 28 U.S.C §1391(b) because Defendant resides within this District, is subject to the court's personal jurisdiction, and maintains its principal place of business within this District.

PARTIES

54. Plaintiff Johnna Battles is a citizen of the State of Alabama. At all relevant times, Plaintiff has been a resident of Rainbow City, Etowah County, Alabama.

55. Defendant, Affinity Cardiovascular Specialists, LLC, is a foreign limited liability company, with a principal address at 4000 Meridian Boulevard, Franklin, Williamson County, Tennessee 37067. At all times material hereto, Defendant, Affinity Cardiovascular Specialists, LLC was doing business as Alabama Cardiology Group, P.C.

CLASS ALLEGATIONS

56. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

57. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class:** All individuals residing in the United States whose PHI/PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant (the "Class").
>
> **Alabama Subclass:** All individuals residing in Alabama whose PHI/PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant (the "Alabama Subclass").

58. Collectively, the Class and Alabama Subclass are referred to as the "Classes" or "Class Members."

59. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

60. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

61. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted in Data Breach.

62. Commonality: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes the following:

a. Whether and to what extent Defendant had a duty to protect the PHI/PII of Plaintiff and Class Members;
b. Whether Defendant had a duty not to disclose the PHI/PII of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendant failed to adequately safeguard the PHI/PII of Plaintiff and Class Members;
d. Whether Defendant required its third-party vendors to adequately safeguard the PHI/PII of Plaintiff and Class Members;
e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI/PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PHI/PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the practices, procedures, or vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

63. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

64. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

65. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

66. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

67. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

68. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

69. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

70. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

71. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

72. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PHI/PII;
c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;
d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PHI/PII;
f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of personal information; and

g. Whether adherence to HIPAA rules and/or other data privacy recommendations and best practices would have prevented the Data Breach.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Classes*)

COUNT 1: NEGLIGENCE/NEGLIGENCE *PER SE*

73. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

74. While providing a health care service, Defendant collects, creates, or shares information about Plaintiff's and Class Members' health status, provision of health care, or payment for health care that can be used to identify Plaintiff and Class Members.

75. Plaintiff and Class Members entrusted Defendant with their PHI/PII with the understanding that Defendant would adequately safeguard their information.

76. Defendant had full knowledge of the types of PHI/PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

77. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PHI/PII, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

78. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology and/or cloud environments; (ii) contractually obligated its vendors to adhere to the requirements of Defendant's privacy policy; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of Defendant's and/or its vendors' data processing activities; (v) regularly audited for compliance

with contractual and other applicable data protection obligations; and, (vi) provided timely notice to individuals impacted by a data breach event.

79. Defendant is a covered entity, as defined by HIPAA and, as such is required to comply with the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E. Under these rules, Defendant had a duty to implement reasonable and appropriate safeguards for the protected health information under its control.

80. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notification no later than 60 calendar days after the discovery of an unauthorized disclosure of unencrypted protected health information. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

81. Defendant breached its duties under HIPAA by failing to conduct regular privacy assessments and security audits; failing to implement reasonable safeguards; and/or failing to timely notify Plaintiff and Class Members of the Data Breach.

82. Defendant also had a duty under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own published privacy policies.

83. Defendant violated Section 5 of the FTC Act by failing to adhere to its own privacy policy regarding the confidentiality and security of Plaintiff and Class Members information.

Defendant further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII.

84. Defendant's violations of HIPAA Privacy, Security and Breach Notice Rules, Section 5 of the FTC Act, and other state consumer protection statutes, constitutes negligence *per se.*

85. Defendant breached its duties, and thus was negligent. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to encrypt PHI/PII in transit and at rest.

b. Failing to adopt, implement, and maintain reasonable administrative, technical, and physical measures to safeguard PHI/PII.

c. Failing to adequately assess the security of its networks and systems.

d. Allowing unauthorized access to PHI/PII.

e. Failing to detect in a timely manner that PHI/PII had been compromised.

f. Failing to destroy or delete PHI/PII it was no longer required to retain.

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

h. Failing to implement data security practices consistent with Defendant's published privacy policies.

86. Plaintiff and Class Members were within the class of persons HIPAA and the Federal Trade Commission Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statues were intended to guard against.

87. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

88. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PHI/PII and the critical importance of protecting that data.

89. Plaintiff and the Classes had no ability to protect the PHI/PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

90. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PHI/PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect the PHI/PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

91. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PHI/PII; (iii) lost or diminished value of PHI/PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their data will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PHI/PII.

92. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

93. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 2: BREACH OF IMPLIED CONTRACT

94. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

95. Defendant creates or collects PHI/PII in the ordinary course of providing products or services.

96. Defendant published a privacy policy to inform the public about how Defendant collects, uses, shares, and protects the information Defendant gathers in connection with the provision of those products or services.

97. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores.

98. Plaintiff and Class Members would not have entrusted their PHI/PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

99. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

100. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendant's web site, privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

101. As a direct and proximate result of the Defendant's breach of an implied contract, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PHI/PII; (iii) lost or diminished value of PHI/PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their data will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PHI/PII.

102. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 3: UNJUST ENRICHMENT

103. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

104. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

105. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit.

106. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

107. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

108. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

109. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 4: INVASION OF PRIVACY

110. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

111. Plaintiff and Class Members had a legitimate expectation of privacy in their protected health information and other personally identifying information such as social security numbers, dates of birth, financial information, and medical information. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

112. Defendant owed a duty to Plaintiff and Class Members to keep their PHI/PII confidential.

113. Defendant permitted the public disclosure of Plaintiff's and Class Members' PHI/PII to unauthorized third parties.

114. The PHI/PII that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PHI/PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

115. Defendant permitted its information technology environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite knowledge of the substantial risk of harm created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

116. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PHI/PII at issue was not newsworthy or of any service to the public interest.

117. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and/or implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

118. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PHI/PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

119. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT 5: DECLARATORY JUDGMENT

120. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

121. Plaintiff and Class Members are consumers of Defendant's products and services. Defendant requires its customers, including Plaintiff and Class Members, to submit PII/PHI in the ordinary course of providing products or services.

122. Defendant gathered and stored the PII/PHI of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII/PHI with the understanding that Defendant would adequately safeguard their information.

123. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

124. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their PHI/PII and remain at imminent risk that further compromises of their PHI/PII will occur in the future.

125. Plaintiff and Class Members have suffered irreparable injury, and will continue to suffer injury in the future, as a result of Defendant's practices, which places Plaintiff and Class

Members at imminent risk that further compromises of their PII will occur in the future. As such, the remedies available at law are inadequate to compensate for that injury. Accordingly, Plaintiff and Class Members also seek to obtain a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure PHI/PII and to timely notify consumers of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various state statutes.

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class Members' PHI/PII.

126. The Court also should issue corresponding prospective injunctive relief requiring that Defendant employs adequate data protection practices consistent with law and industry standards.

127. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

128. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the multitude of individuals whose PII would be at risk of future unauthorized disclosures.

129. As a result of the Defendant's data security practices, the consuming public in general, Plaintiff, and Class Members suffered injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and

available for unauthorized third parties to access; and (b) remains under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

130. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web monitoring and/or identity theft and fraud protection to all affected by the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statues and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: September 6, 2024.

By:*/s/Roy T. Willey*
Roy T. Willey, Esq. (TN Bar No. 41046)
Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
roy@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff
**Pro Hac Vice forthcoming*